(12) UK Patent Application (19) GB (11) 2 386 710 (13) A

(43) Date of A Publication 24.09.2003

(21) Application No 0206399.8

(22) Date of Filing 18.03.2002

(71) Applicant(s)
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto,
California 94304, United States of America

(72) Inventor(s)
Simon Shiu
Adrian Baldwin
Marco Casassa Mont

(74) Agent and/or Address for Service
Hewlett-Packard Limited
Intellectual Property Section, Building 3,
Filton Road, Stoke Gifford, BRISTOL,
BS34 8QZ, United Kingdom

(51) INT CL[7]
G06F 1/00

(52) UK CL (Edition V)
G4A AAP

(56) Documents Cited
EP 0192243 A2 **WO 2000/079368 A1**
WO 2000/025214 A1 **WO 1996/005673 A1**

(58) Field of Search
UK CL (Edition T) **G4A AAP**
INT CL[7] **G06F 1/00**
Other: **Online: EPODOC, WPI, PAJ, TDB, XPESP, INSPEC, EXPLORE**

(54) Abstract Title
Controlling access to data or documents

(57) A method for access to data or documents receives the document or data in encrypted format, receives access policy data relating to the data or document, reads the access policy data and verifies individual conditions specified in the access policy data, and allows decryption of the data or document if the conditions are successfully verified.

The method uses a secure control apparatus which includes a key escrow component to safeguard private keys. There may also be a policy enforcement and key management device in a separate tamper-proof casing, the device preferably including a communications port, a policy enforcement component, an identification component and a tamper detection component.

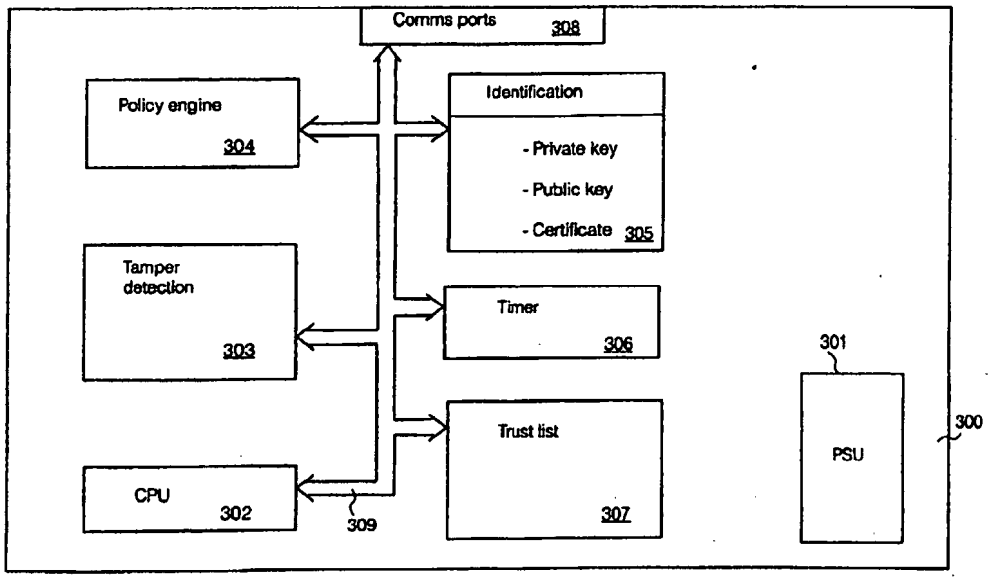

Fig. 3

GB 2 386 710 A

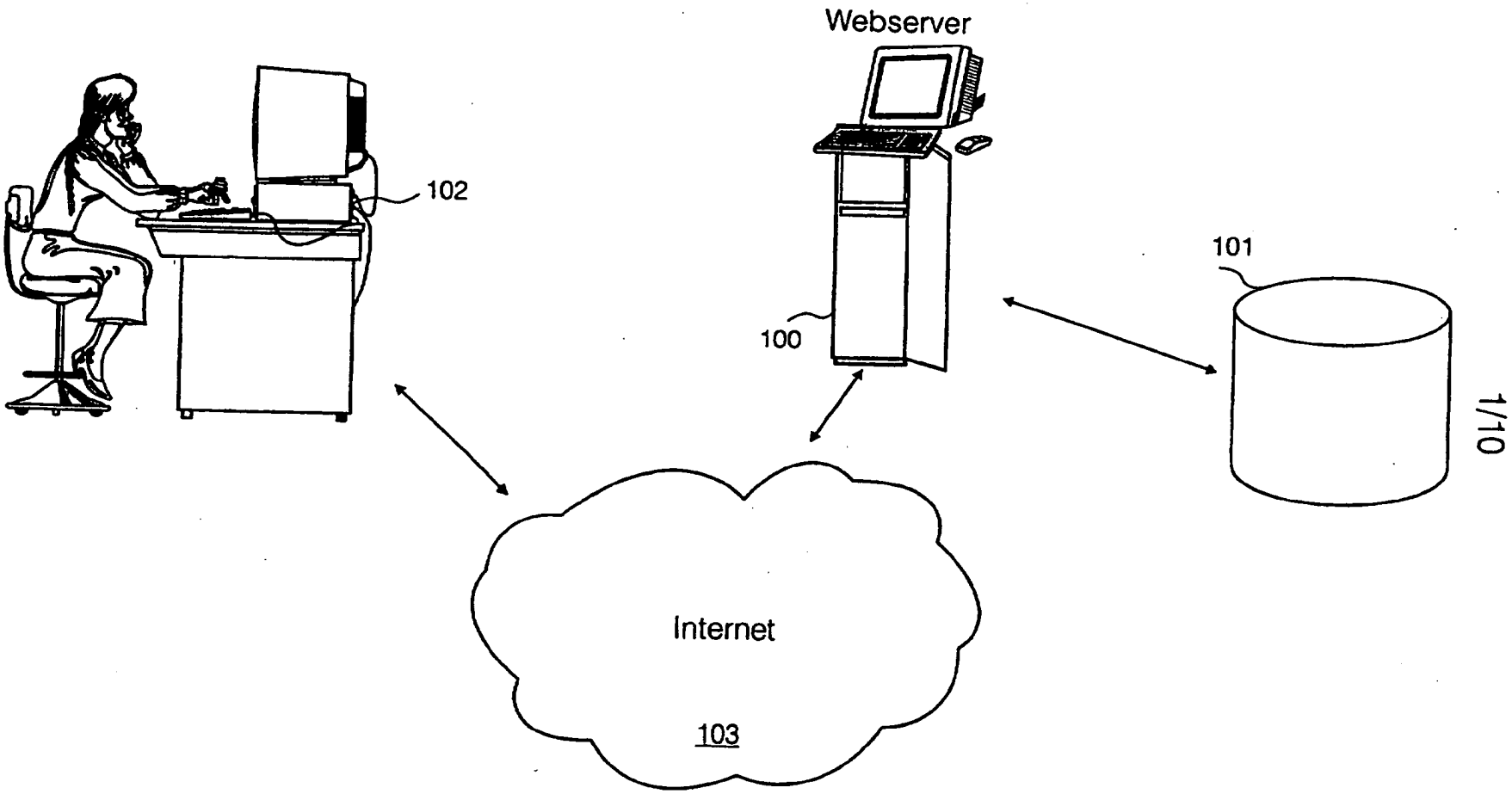

Fig. 1
(Prior Art)

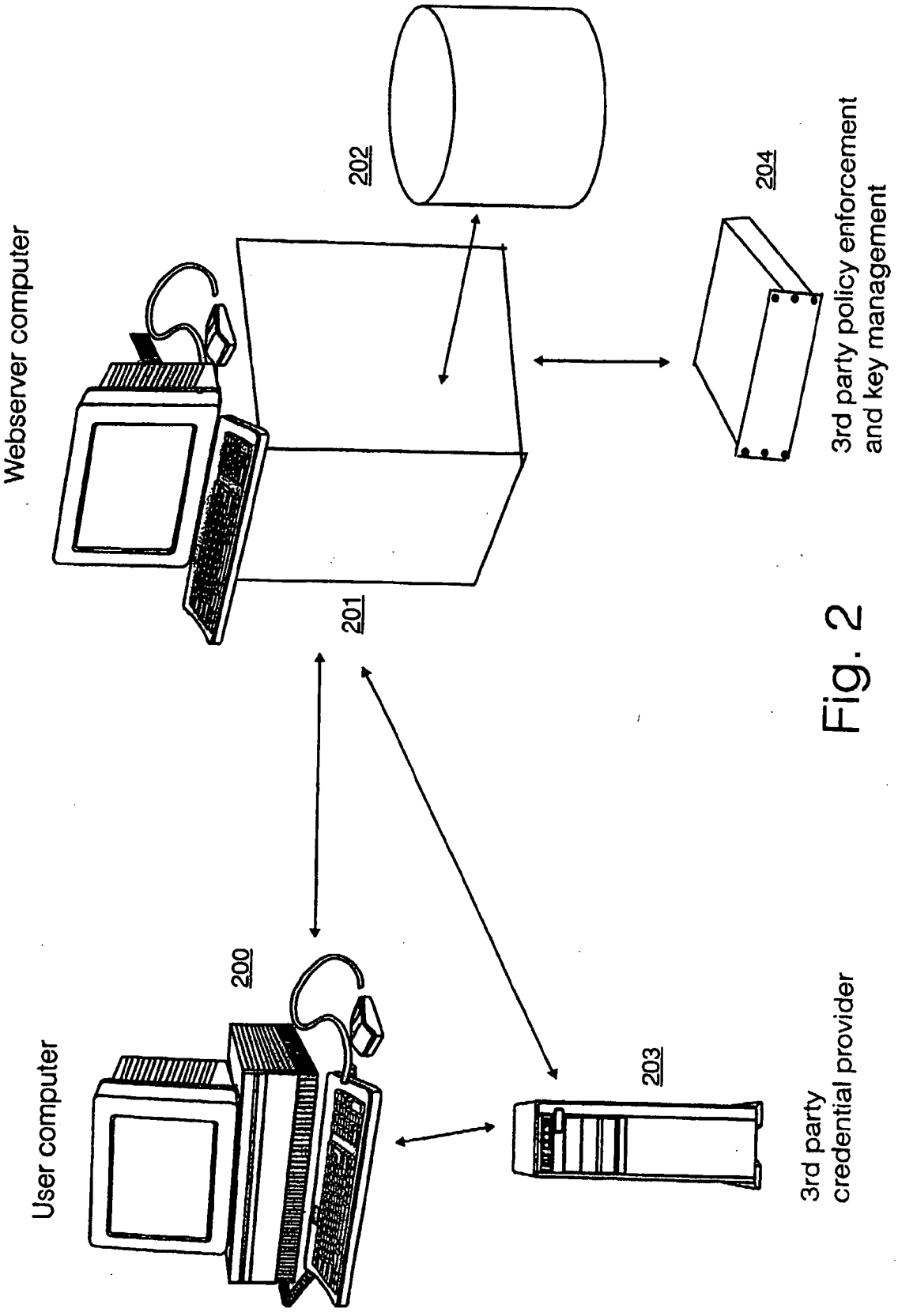
Webserver computer
202
204
3rd party policy enforcement and key management
201
User computer
200
203
3rd party credential provider

Fig. 2

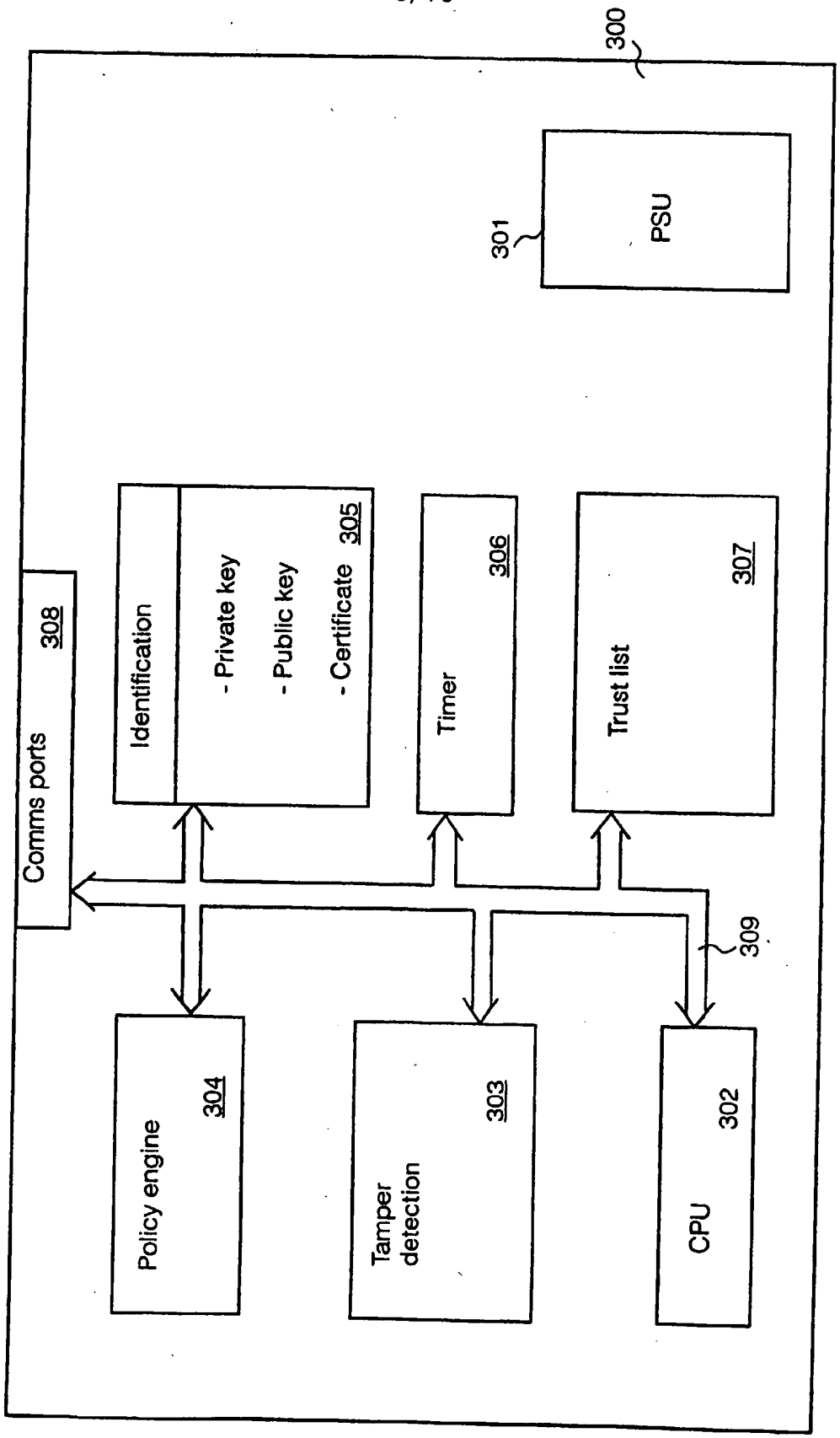
300
301
PSU
Identification
- Private key
- Public key
- Certificate
305
Timer
306
Trust list
307
Comms ports
308
309
Policy engine
304
Tamper detection
303
CPU
302

Fig. 3

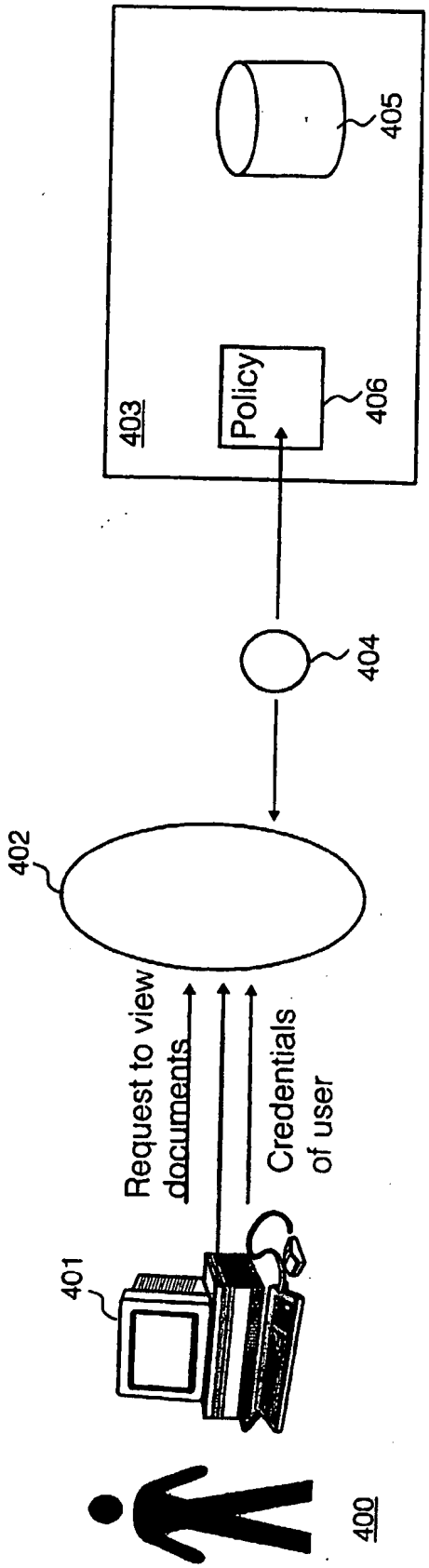
405
403
Policy
406
404
402
Request to view documents
Credentials of user
401
400

Fig. 4

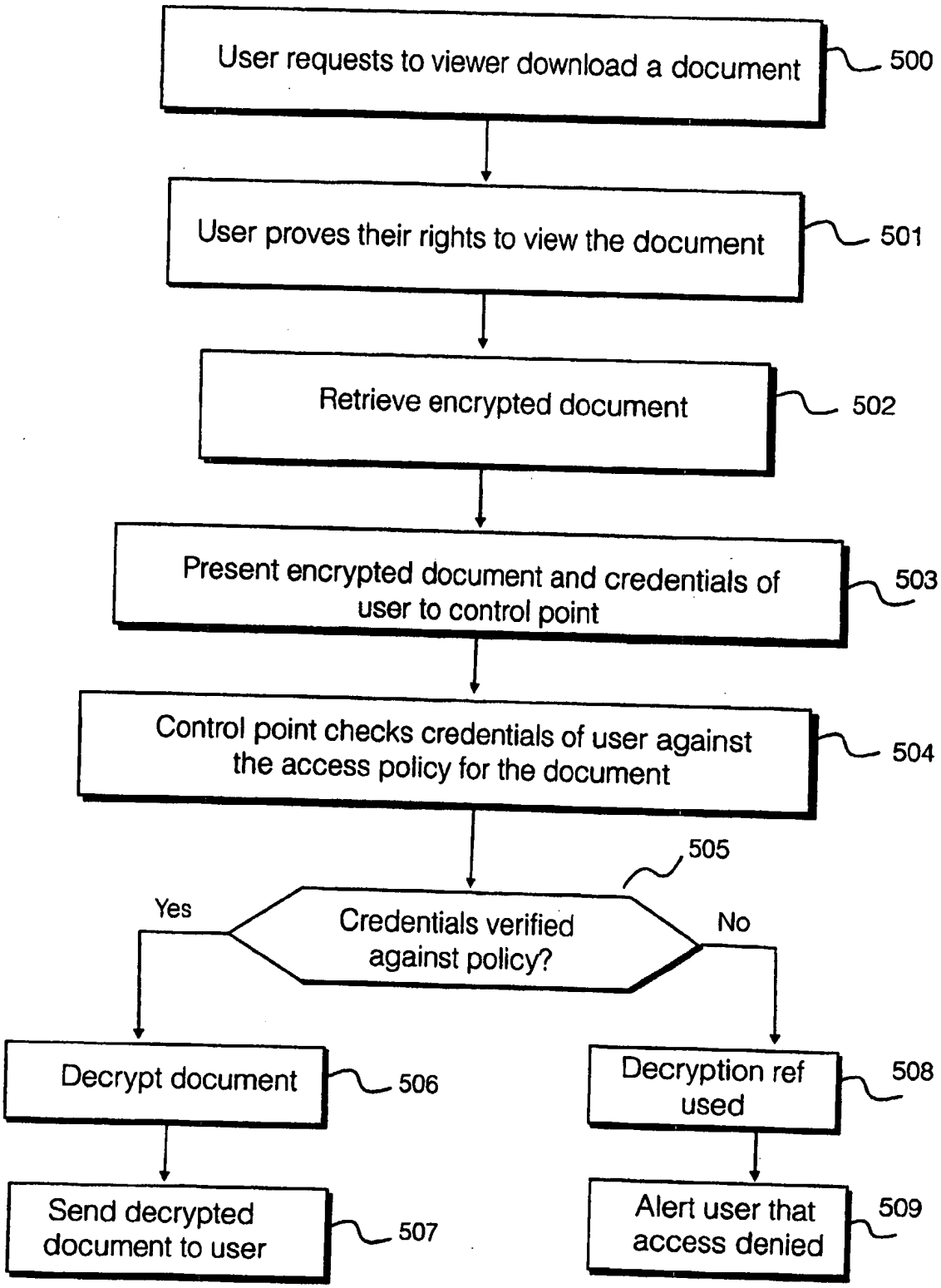
User requests to viewer download a document
500
User proves their rights to view the document
501
Retrieve encrypted document
502
Present encrypted document and credentials of user to control point
503
Control point checks credentials of user against the access policy for the document
504
505
Credentials verified against policy?
Yes
No
Decrypt document
506
Send decrypted document to user
507
Decryption ref used
508
Alert user that access denied
509

Fig. 5

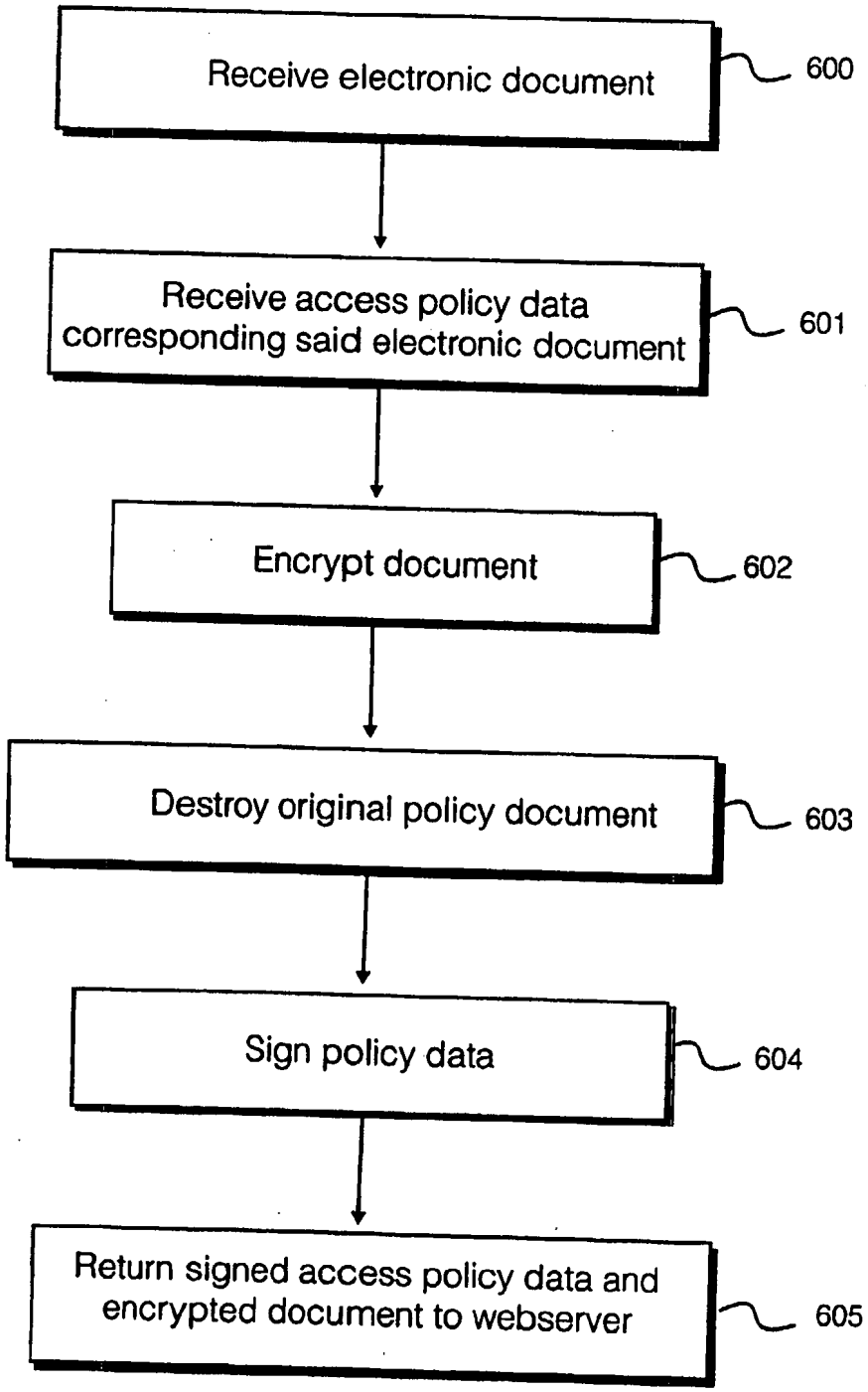
Receive electronic document
600
Receive access policy data corresponding said electronic document
601
Encrypt document
602
Destroy original policy document
603
Sign policy data
604
Return signed access policy data and encrypted document to webserver
605

Fig. 6

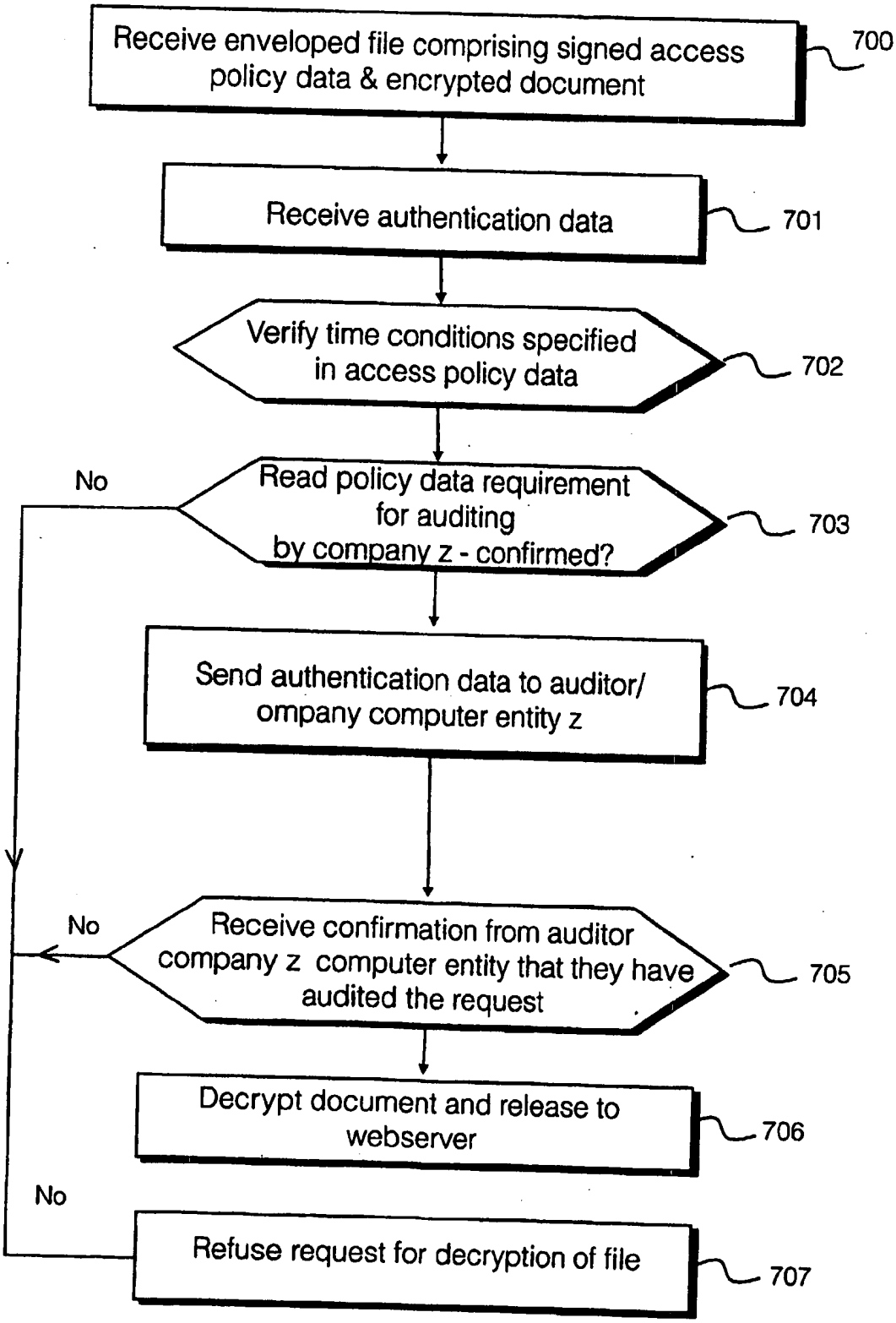
Receive enveloped file comprising signed access policy data & encrypted document
700
Receive authentication data
701
Verify time conditions specified in access policy data
702
No
Read policy data requirement for auditing by company z - confirmed?
703
Send authentication data to auditor/ ompany computer entity z
704
No
Receive confirmation from auditor company z computer entity that they have audited the request
705
Decrypt document and release to webserver
706
No
Refuse request for decryption of file
707

Fig. 7

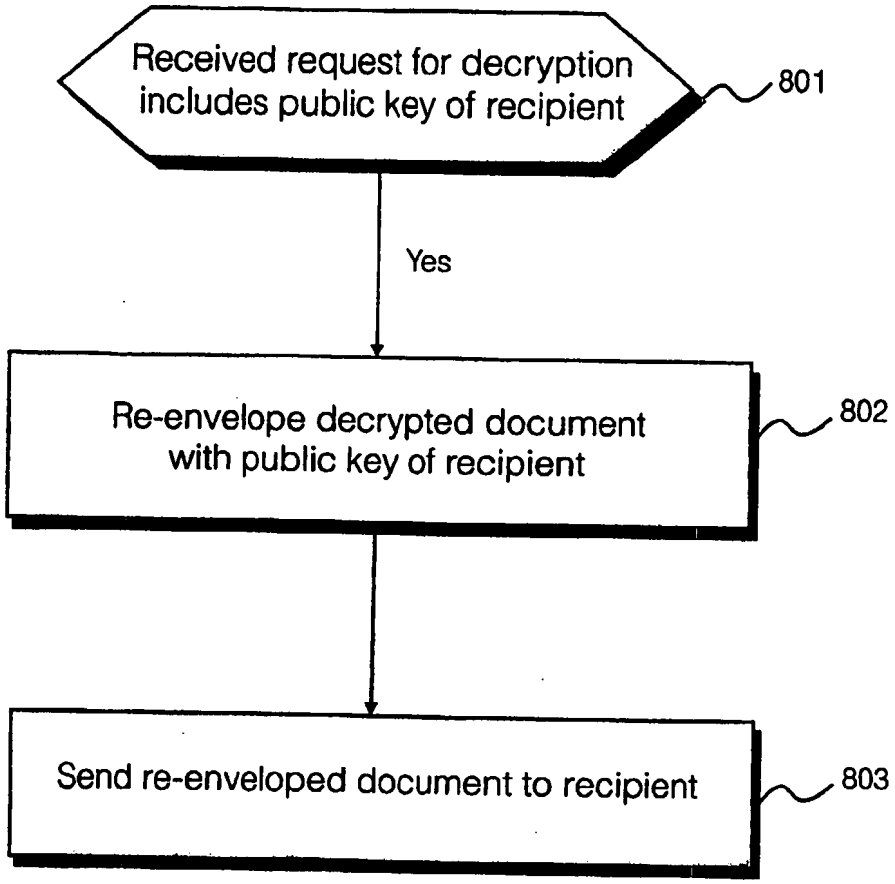
Received request for decryption includes public key of recipient
801
Yes
Re-envelope decrypted document with public key of recipient
802
Send re-enveloped document to recipient
803

Fig. 8

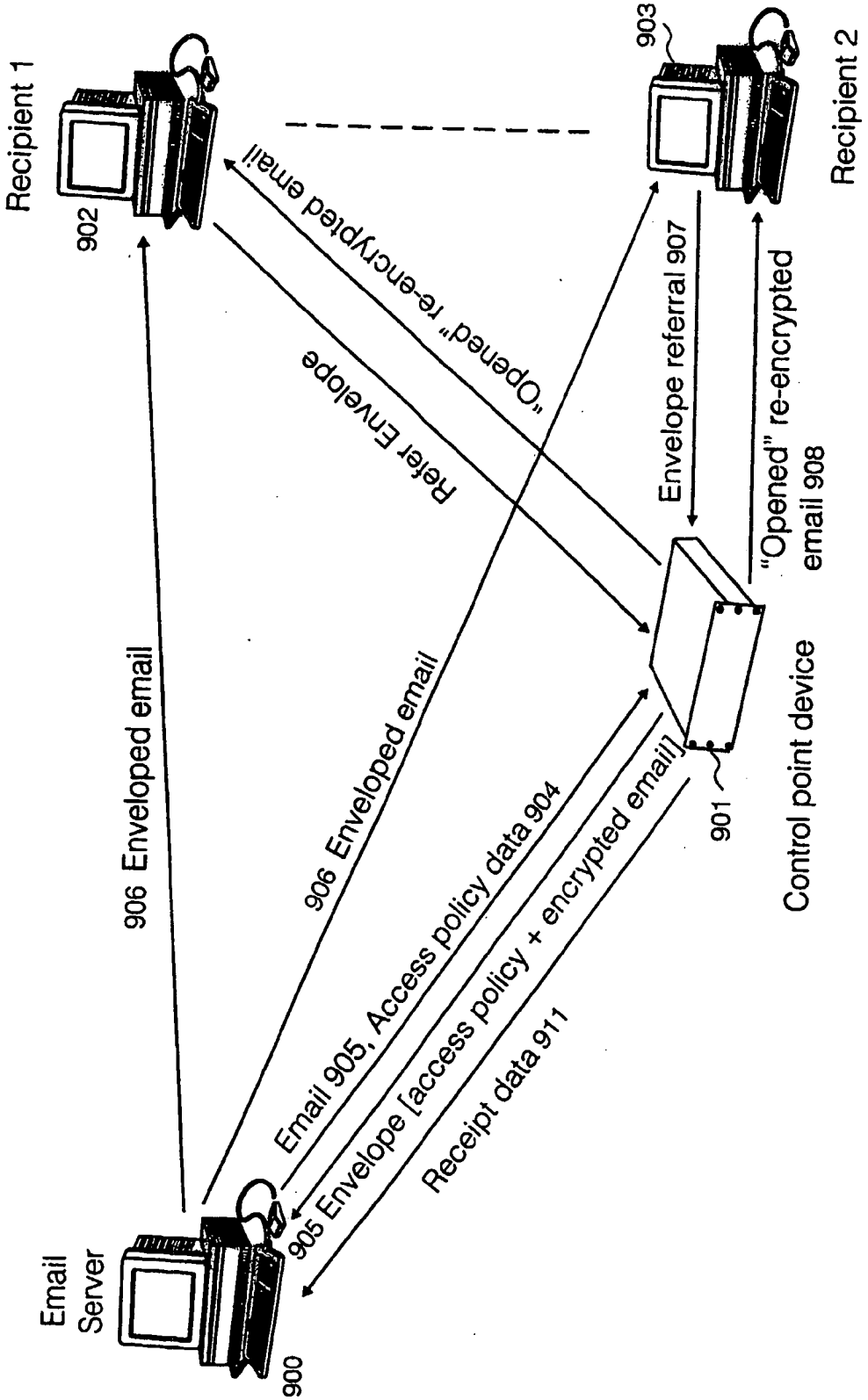
Recipient 1
902
903
Recipient 2
"Opened" re-encrypted email
Refer Envelope
Envelope referral 907
"Opened" re-encrypted email 908
906 Enveloped email
906 Enveloped email
Email 905, Access policy data 904
905 Envelope [access policy + encrypted email]
Receipt data 911
Email Server
900
901
Control point device

Fig. 9

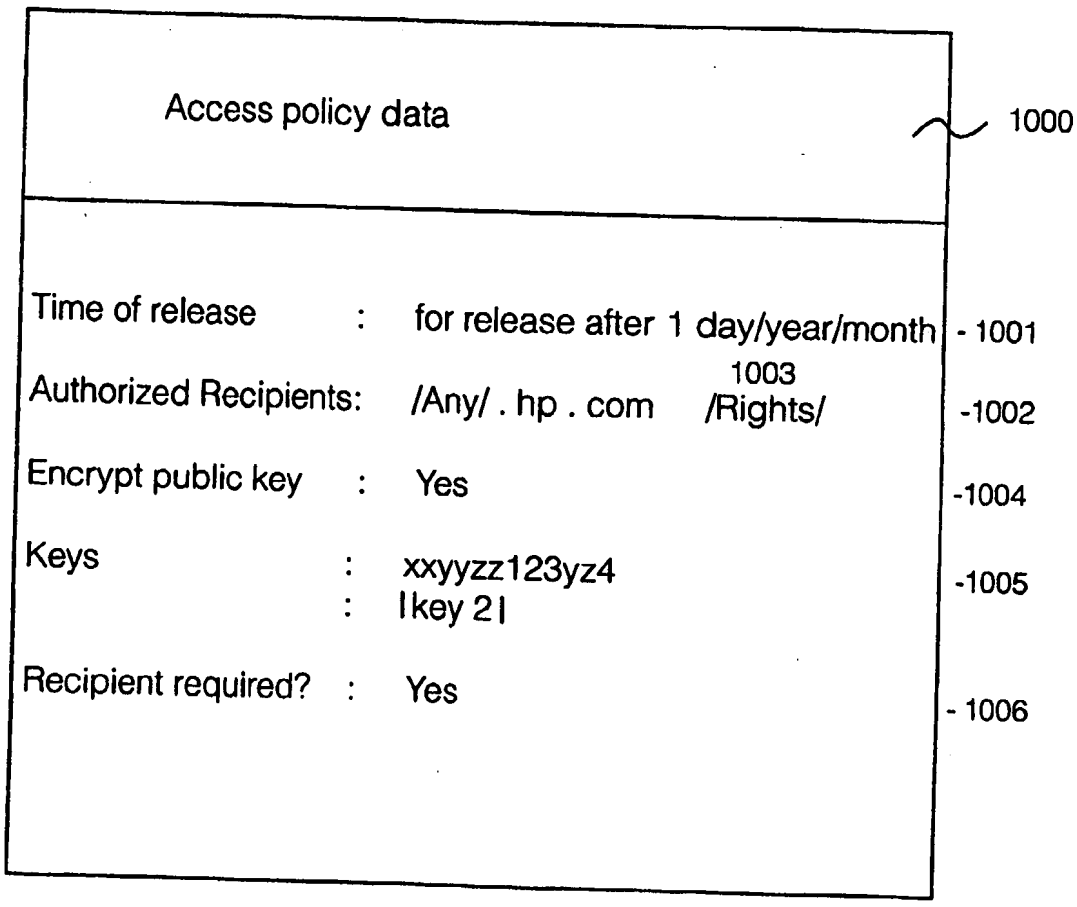
Access policy data
1000
Time of release : for release after 1 day/year/month
- 1001
Authorized Recipients: /Any/ . hp . com
1003
/Rights/
-1002
Encrypt public key : Yes
-1004
Keys : xxyyzz123yz4
: Ikey 2I
-1005
Recipient required? : Yes
- 1006

Fig. 10

2386710

ENSURING POLICY ENFORCEMENT BEFORE ALLOWING USAGE OF PRIVATE KEY

Field of the Invention

The present invention relates to security in computing systems, and particularly although not exclusively, to a method and apparatus for controlling access to documents.

Background to the Invention

In most prior art computer data storage solutions, for most documents, access control is enforced by an operating system structure, i.e. files are not encrypted, and so the issue of key management does not arise. Current prior art solutions concentrate on how and where to enforce a policy, or on protecting a private key.

Prior art systems for keeping a private key private address this problem in some instances by use of a tamper proof cryptographic box. An example of such a tamper proof cryptographic box can be found in the prior art by nCipher (www.nCipher.com). The nCipher system contains a Java Virtual Machine (JVM) and has a secure way to deploy Java solutions in the same way as a conventional generic computer device can be applied to any computer problem, the nCipher tamper proof cryptographic box can be applied to various cryptographic services. In practice, apart from protecting a private key, the nCipher system is intended to restrict the keys usage by enforcing a strict API.

In EP 1022640, a time stamp service is disclosed, which also discloses controlling how, when and where a private key can be used.

WO 00/122650 discloses a server side implementation of a cryptographic system. The system disclosed is concerned with making a server a control point, and dealing with private key usage.

In WO 95/19672, there is disclosed a cryptographic system with key escrow feature. This system has a control point, and a key which will only be used when it is satisfied that certain escrow features are met.

WO 01/22242 discloses a data providing system and method. This system describes delivery of media data together with policy information determining who can view the media data. Both policy and content data are encrypted, and policy data is decrypted by an end point which will only decrypt content data if the policy is satisfied.

US 5742682 discloses a method of manufacturing secure boxes in a key management system. The system disclosed concerns a protocol for safely manufacturing secure boxes with private keys.

WO 0152471 discloses a black box for digital rights management system. The black box is used to enforce rights to a document.

Specific implementations according to the present invention address the problem of how to access a plurality of encrypted documents stored in a data storage device, and how to control which users are able to access which encrypted documents.

Summary of the Invention

Specific implementations according to the present invention enable management of access control to encrypted documents by using control points and trusted third parties to tightly couple policy enforcement with usage of one or more private keys required to decrypt a document. In use, a user submits a document together with policies for management of that document for retrieval to a control point. The control point returns a signed version of the policy and an encrypted and/or enveloped version of the document. The control point only decrypts or releases the document provided that an accompanying signed and trusted policy requirement has been satisfied.

The control point and/or trusted third party can be designed to be stateless, which enables the control point to be delivered as a tamper proof cryptographic box. This in turn means that the access control service can be used in a scalable way to manage complex access control issues. It also enables increased confidentially from the third party.

According to a first aspect of the present invention there is provided a method of controlling access to data stored in a database, said method comprising:

providing a secure control apparatus, said apparatus comprising a policy enforcement component for enforcing at least one data access policy to said database and a key escrow component for ensuring a set of private keys remain secure;

connecting said secure control apparatus to a web server computer entity, said web server computer entity configured for storing a plurality of encrypted files;

upon receipt of a request to access a said encrypted file, received by said web server computer entity, said secure control apparatus operating to; check for an access policy applicable to said requested file;

establish an identity of said entity requesting said file;

if said entity has an identity which, according to said access policy, is authorised for accessing said file, then releasing said file for access to said computer entity; and

if said computer entity requesting said file does not have an identity which, according to said access policy is authorised for accessing said file, then denying access of said file to said requesting computer entity.

According to a second aspect of the present invention there is provided there is provided a document management service comprising:

receiving a document;

receiving an access policy data describing an access policy applicable to said received document;

encrypting said document;

signing said access policy data with a digital signature of a secure device.

According to a third aspect of the present invention there is provided a method for enforcement of an access policy applicable to a document, said method comprising:

receiving said document in encrypted format;

receiving an access policy data applicable to said encrypted document;

reading said access policy data;

verifying individual conditions specified in said access policy data;

if said individual conditions are successfully verified, then allowing decryption of said received document: and

if said individual policy requirements are not verifiable, then generating a message indicated that said encrypted document is not permitted to be accessed.

According to a fourth aspect of the present invention there is provided a policy enforcement and key management device, said device comprising:

a tamper proof casing;

at least one communications port for sending and receiving electronic data; and

means for reading an access policy data; and

means for applying an access policy to a document, according to said access policy data.

According to a fifth aspect of the present invention there is provided a method for providing a service for enforcement of access policies applicable to a plurality of documents, said method comprising;

receiving at least one said document in encrypted format;

receiving at least one access policy data applicable to said encrypted document;

reading said access policy data;

determining whether a set in criteria specified in said access policy data are satisfied for said encrypted documents; and

if said set of criteria are satisfied, then decrypting said document; and making said decrypted document available to a user of said service.

Further technical features of the invention are as recited in the claims herein.

Brief Description of the Drawings

For a better understanding of the invention and to show how the same may be carried into effect, there will now be described by way of example only, specific embodiments, methods and processes according to the present invention with reference to the accompanying drawings in which:

Fig. 1 illustrates schematically a prior art system for accessing encrypted documents;

Fig 2. illustrates schematically a first system for secure storage of documents which are remotely accessible, and in which access policy enforcement and key management are applied by a stand alone computer entity device according to a first specific implementation of the present invention;

Fig 3. illustrates schematically an architecture and components of a policy enforcement and key management device according to a second specific implementation of the present invention;

Fig 4. illustrates schematically an overall method of operation of the system of Fig. 3;

Fig. 5 illustrates schematically by way of process steps, an overall operation of the system of Fig. 2;

Fig. 6 illustrates schematically operation of the policy enforcement and key management device of Fig.3 in a specific mode of operation for encrypting a document and using an envelope file for passing back to a web server device for storage in a database;

Fig. 7 illustrates schematically a specific mode of operation of the policy enforcement and key data management device of Fig.3 for enforcing a specific example of an access policy data attached to an encrypted document;

Fig. 8 illustrates schematically a method for re-enveloping a decrypted document prior to sending to an authorised recipient;

Fig 9. illustrates schematically a second system, according to a second specific implementation of the present invention, for storage and management of e-mails, in which access policy enforcement and key management are controlled by a stand alone policy enforcement and key management device; and

Fig. 10 illustrates schematically an example of an access policy data attaching to an e-mail document in the system of Fig 9.

Detailed Description of the Best Mode for Carrying Out the Invention

There will now be described by way of example the best mode contemplated by the inventors for carrying out the invention. In the following description numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent however, to one skilled

in the art, that the present invention may be practiced without limitation to these specific details. In other instances, well known methods and structures have not been described in detail so as not to unnecessarily obscure the present invention.

In this specification the term "entity" when generally used is to be taken as including any type of entity which is capable of sending or receiving documents and includes computer devices, corporate bodies, governmental organizations, intergovernmental organizations, legal persons and natural persons. Entities as referred to in this specification may have identities, as evidenced by digital certificates issued to those entities.

In this specification, the term "computer entity", is used to refer to a device having data processing capability and memory, and electronic communications ability for communicating with other computer entities. A computer entity may be owned by, be operated by or represent an entity as described in the preceding paragraph.

Specific embodiments disclosed herein relate to specific problems as follows:

- firstly, the need to control the usage of a private key; and
- secondly, managing the enforcement of policies for access rights.

A solution is disclosed whereby a single control point, which could be a third party run service, is used to authenticate and/or validate an access policy, and to encrypt and decrypt a document. The solution uses asymmetric cryptography, specifically a private key to enforce both encryption and decryption, and authentication and validation of the access policy. The service can be designed to be stateless, so that it can be delivered via a tamper proof cryptographic box. This makes manufacture and distribution of such control points much more flexible and so aids the scalability of the solutions disclosed. It also ensures that a service provider does not have access to the documents, or even access to

requests for access to documents. This is an added benefit for increasing confidentiality.

A cryptographic box device is given a document and a policy concerning access rights to that document. The cryptographic device signs the policy, encrypts and/or envelopes the document, and returns both the encrypted/enveloped document and the signed policy back to a user or a users application. The user application stores the returned data and destroys the original document. From then on, the only way to recover the document is to pass the returned encrypted/enveloped data together with the appropriate authentication information back to the cryptographic box.

The box does not need to hold any state with respect to these transactions. That is to say, the control point device does not need to remember or store any information regarding a document which the device has encrypted, or an access policy which the device has signed, and can "forget" about the document and policy. The device does however, need to maintain a state with respect to its own identity, that is , to store its own digital certificate and public and private.

The device does however need a way to interpret and validate the authentication information. In various embodiments, this is achieved by configuring the box to trust specific identified service providers, by including the public key of such providers in a "trusted provider" table, which will validate authentication information against a policy statements, and will sign, in a manner verifiable by the box, that it has checked it. Alternatively, the service and/or cryptographic box could have a relationship with a number of credentials providers and/or time stamp authorities, so that it can directly cross check the authentication information with the policy and form judgements by itself.

To avoid disclosure of a private key to the cryptographic control point device, a protocol is used to manufacture a set of such boxes with a same private key (which may in itself enhance scalability), or to escrow the key.

In best mode implementations, XML can be used as an underlying format, to tie together the document, policy and authentication information at various points in the system.

Example 1

A third party document management service may assure customer confidentiality of stored documents by encrypting them. Each document is likely to have a unique access rights based on the policies of many customer corporations. An example of an access policy maybe:

i) access only allowed after a particular date, for example January 22 2002;

ii) a request must have credentials from a specified company X showing that they have purchasing rights, or that they are from a second specified company Y and have selling rights;

iii) the request must audited by a third company Z.

It is assumed that these policies are stated and arrive with the document. The policy and the document are passed to a cryptographic box which, in the case of the standard PKI model, encrypts the document and signs the policy information. The service may also destroy the original document, so that the only way to recover the original document is to submit the document with its signed policy as part of the document, together with authentication information, which will satisfy the policy requirements. For example for the above case;

1. the service has access to a trusted clock, so that the service can verify the time conditions;

2. the service trusts the credential providers for company X and company Y, and knows their public keys, and therefore can verify the credentials presented;

3. the service sends a copy of the request to the company Z, and only releases the document when the company Z confirms that they have audited the request.

For additional privacy, a request for decryption could also contain a public key of an intended recipient, so that the cryptographic box can re-envelope the documents specifically for that user.

Referring to Fig. 1 herein, there is illustrated schematically one example of a prior art system for storage of encrypted documents which are remotely accessible. A web server 100, which has an associated database 101, is accessed by a user computer 102 over communications network 103 for example the internet.

The user accesses the web server via a known portal, and web browser software. A plurality of electronic data records stored in the database are each encrypted. There are therefore two problems in serving the documents to a user requesting those documents. Firstly, the documents have to be decrypted before they are sent to the user. Secondly, access control policies need to be enforced, so that the data documents are only recoverable by authorised users.

The user logs into the web server, using a browser, and makes a request to view a document. The web server 100 needs to determine that the user is an authorised user, before releasing a document, and needs to decrypt that document, or allow the user to decrypt the document, so that the user can read the content of the document.

In the prior art, the point at which the point at which the proof of the user is determined is within the web server 100. This is in a different position, to the place where encryption keys are stored.

Referring to Fig. 2 herein, there is illustrated schematically a system for secure storage of documents, which are remotely accessible which operates by ensuring policy enforcement before allowing usage of a private key according to a specific implementation of the present invention.

The system comprises a user computer entity 200 having a known web browser, through which a user can access web sites; a web server computer 201, the web server computer running a web site application; a database 202, the database storing encrypted data files, and communicating directly with the web server computer over a secure channel; a third party credential provider 203, for providing digital certificates identifying computer entities; and an enforcement and key management apparatus 204 for ensuring enforcement of policies for allowing access to encrypted documents, and for providing key management, allowing access to decryption capability for decrypting encrypted documents stored in the database 202.

Referring to Fig. 3 herein, there is illustrated schematically a policy enforcement and key management device. The device comprises a secure tamper proof casing 300 containing a power supply unit 301; a central processing unit 302 in the form of a known data processor device; and a plurality of firmware modules comprising a tamper detection module 303 for detecting whether the device has been tampered with; a policy engine 304 for enforcing data control policies for accessing data, an identity module 305 comprising means for generating one or a plurality of private keys, one or a plurality of public keys, and a digital certificate identifying the device; a secure timer device 306 capable of maintaining a device time; a trust list 307 comprising a list of pre-stored addresses of trusted computer entities with which the device can comuniate, a communications port 308; and an internal bus 309 linking the components.

According to a specific method of the present invention, both policy enforcement and protection of encryption keys is carried out by a single computer entity, the policy enforcement and key management device 300, for allowing access of users to the electronic database 202 storing encrypted documents. The policy enforcement and key management device provides a single control point for controlling access to encrypted data records stored in a database. The control point may be provided as a service to an operator of a web server computer 201, or may be provided as a bought item, which an operator of the web server computer purchases, and links to their web server computer to provide access to that web server computer.

Referring to Fig. 4 herein, there is illustrated schematically a logical diagram showing policy enforcement and access control according to a specific method of the present invention. A user 400 operator user computer entity 401, comprising a conventional web browser, which, via an internet portal 402, provided by an internet service provider, contacts a web server computer 403, with an identity of the user 400 being router through a single control point 404, provided by a policy enforcement and key management device as described with reference to Figs. 2 & 3 herein. A request to see a particular document stored in database 405 is made by the user 400 in order to access that document, a policy 406 is in force, specifying for example, that the user 400 needs to prove their identity prior to accessing the document, for example, where encrypted document stored in the database 405 are confidential patient health records, the policy 406 may specify that only qualified doctors may access those confidential patient health records. Therefore, in order to access the document, the user 400 needs to prove that they are a doctor, enforcement of the policy 406 is carried out at the control point 404, by establishing the identity of the user. Although the policy may be contained locally at the web server computer entity, enforcement of the policy is controlled in a separate device at a control point 404 separate from the web site.

Referring to Fig. 5 herein, there is illustrated schematically an overall process carried out by the system of Fig. 4.

In step 500 a user requests to view or download a document from the website. A decision as to who accesses the database, as well as protection of a private key for decrypting the document is controlled by the control point.

The user must prove that the have rights to view the document. The credentials of the user are transmitted along with the request to view the document. The website retrieves the encrypted document in step 502 and in step 503 presents the encrypted document, along with the credentials of the user to the control point 404. The control point checks the user credentials against the access policy for that document, and in step 505, if the control point determines that the user credentials are verified, and that user of a user of that type is permitted to access that document, then in step 506 the document is decrypted and the decrypted document is sent by the control point to the user in step 507.

However, if the credentials of the user are not verified, or if a user having those credentials is denied access to the encrypted document by the access policy enforced for that document, then decryption is refused in step 508, and in step 509 the user is alerted that access to the document is denied.

Referring to Fig 6. Herein, there is illustrated schematically processed steps carried out by the policy enforcement and key management device for providing an encrypted document having attached policy access data. The device receives an electronic document from a web server computer in step 600, along with an associated access policy data corresponding to the electronic document in step 601. In step 602, the device encrypts the document. Optionally, after encryption, the original policy document may be overwritten within the device, so that the only way of retrieving the document is to decrypt the encrypted document, which will require the device to perform further operations when presented with that encrypted document by a computer entity referring the document to the device

again. In step 604, the policy data is signed, and in step 605, the signed access policy data and encrypted document are returned to the web server which originally sent the electronic document and policy data the device. The signed policy access data and encrypted document are provided within an electronic envelope, and returned to the web server.

The web server computer entity can store the enveloped data file in the database. Any person attempting to access the database, cannot read the documents since it is encrypted. Further, any person requesting access to the documents including encryption, must satisfy the criteria for the access policy described by the access policy data comprising the file.

Referring to Fig. 7 herein, there is illustrated schematically operations carried out by the policy enforcement and key management device for releasing an enveloped data file in response to a request for release of the enveloped file from a web server computer entity. In step 700, the device receives the enveloped file comprising the signed access policy data and the encrypted document, from the web server. The web server may receive a request to access the document from a user computer via the web servers web interface (website), and in response, the web server computer retrieves the enveloped file from the database, and sends it to the device. Additionally, the web server must collected authentication data from the user requesting a copy of the file, and passes this one to the device as well. The device receives the authentication data in step 701 and in step 702 sends the authentication to a computer entity of an auditor company Z, which is specified in the access control policy as being required to audit a request for a document before a document is released. This step is specifically carried out in response to part of the access control policy data. In step 702, the device reads the policy data, and reads a requirement contained within the policy data that any requests for access to the document must be sent to an auditing company Z for approval.

In step 703, the device reads from the access policy data that there is a time conditions applicable to the document, that is, the document is only accessible after a particular date. The device checks with its internal timer device to see if the date has been reached yet, and if so, can continue to process the file. If the time condition is not satisfied, then the device refuses the request for access to the file in step 707.

If in step 705, the device received confirmation from the auditor company's computer entity, that they have approved the request, then in step 706 the document is decrypted and is returned to the web server computer. The web server computer may then send the document to the requesting user, or allow the requesting user to view the document over the website.

In the example shown in Fig. 7, in order to gain access to a protected file, a user must satisfy the enforcement and key management device as to the identity of the user, and also the device reads the policy data and applies enforcement of the policy by, in this example, checking that the document is beyond a release date specified in the policy data for release of the document, and also by receiving confirmation from a third party company Z who audits all requests to access the document, that the user is a person authorised to access that document.

Referring to Fig 8. herein, on receiving a request for access to a decrypted document, the policy enforcement and key management device may provide the document, re-enveloped for a particular intended user, provided that the device receives the public key of the intended user recipient.

In step 801, the policy engine of the device checks an incoming message from the web server computer entity to see if a public key of an intended user recipient device is included. If the public key is included, then in step 802 the policy engine of the device re-envelopes the decrypted document, by encrypting it using the public key of the recipient user device. The policy enforcement and key

management device may then send the re-envelope document directly to the recipient user device in step 803.

Example 2

Referring to Fig 9. Herein A second example implementation according to the present invention provides a third party e-mail messaging service. Convention email, although immensely effective as a messaging service, lacks many desirable properties such as assured delivery, receipting, and timed release. These properties can be provided by using an intermediary device which holds a message and records when the message is accessed and by whom. The cryptographic control point disclosed herein may form the basis of a third party service for providing timed release of documents, or receipting of documents and short delivery.

A sender submits a message, and submits conditions under which the message may be released to the cryptographic service. The cryptographic service signs the conditions and encrypts the message. The cryptographic service only decrypts the message when it is satisfied that the specified conditions have been met. If the sender is concerned about the security of the email, then the sender may delete the original unencrypted email, once an encrypted version has been made by the cryptographic control point. From then on, where the sender destroys the original document, the only way of recovering the original unencrypted email is for the control point device, (or another equivalent control point device trusted by the control point device which originally encrypted the email) to decrypt the email in accordance with the access control policy specified in an electronic envelope containing the encrypted email.

The service may be embodied as a stand alone secure equipment, and may be lent by a third party to a sender, thereby giving more assurance to the sender that no one except the intended recipients can see the message, not even the third party itself. The box apparatus may sign receipts and if appropriate sign time stamps depending on the level of evidence required from

the third party. The equivalent box may be returned, and if intact, the third party may vouch for those receipts.

One advantage of the service is that it involves a third party controlling the release or offering audit and receipting of documents. An advantage of the service is an extra level of control and ownership for users that the box delivery mechanism allows.

Referring to Fig 9 herein, there is illustrated schematically a system for secure email transmission comprising an email server 900 operable for sending emails; a policy enforcement and key management device 901, for enforcing the an access control policy attaching to one or more emails, and a plurality of receiving entities 902, 903. The e-mail server 900 has an associated database 903, for storing e-mails as document files. The e-mail may be intended for one or more ultimate recipient devices 902, 903. The sender may specify that individual intended recipients can view the e-mail. This information is contained in an access policy data 904 forwarded to the e-mail server along with the e-mail file 905. The access policy data may also specify items such as a timed release of information. For example a sender of the e-mail may wish the e-mail to be viewable on or after a specified time and date. For example where the e-mail comprises a research paper, where the release of the research paper needs to be timed to occur after another event, for example filing a patent application for the same material, the sender of the e-mail may wish to prepare the document for viewing in advance, but delay actual viewing of the document until a specified time and date. This delay can be specified in the access policy data 904.

Similarly, where the e-mail contains commercially sensitive information, for example company financial results, and those financial results need to made available at a particular time, to coincide with release of data according to stock market rules, the sender may specify within the access policy data 904, the time

and date on which those documents may be viewed, together with specifying the intended recipient devices to whom access of the document will be allowed.

Enforcement of the access policy is made via a policy enforcement and key management device 901, acting in a role as a control point for allowing access to the e-mail and allowing distribution of the e-mails to intended recipients.

Referring to Fig. 10 herein, there is illustrated schematically an example of an access policy data sent by the e-mail server, specifying access criteria to be applied to the e-mail document. The access policy data comprises a time field 1001 specifying a time after which the document can be made available for viewing and/or release; an authorised recipient field 1002, containing data describing one or more authorised recipient devices, and/or one of more authorised recipient users who are to be able to have access to view the document, the authorised recipient field may also contain a 'rights' field 1003 specifying, for each individual authorised recipient, or for each class of authorised recipient, a type of access right to the e-mail which is permitted, for example 'view only', or 'view and download'; a delivery method field 1004, specifying deliver criteria such as whether the document should be delivered encrypted with a public key of an intended recipient; a key field 1005 containing public keys of intended recipients, and to be used for encrypting the e-mail with a public key where the delivery mode field 1004 specifics public key encryption; and a receipt field 1006 specifying whether a receipt is to be generated upon delivery of the e-mail document to an intended recipient.

The email server submits an email message including conditions under which the message may be released, to the control point device 901 . The control point device 901 proceeds to encrypt the e-mail, and to sign the access policy data. The control point device then returns an enveloped file to the e-mail server 900. The control point device 901 does not store the original e-mail after it has enveloped it. Once it has encrypted the e-mail and sent it back to the e-mail

server 900, it does not send the original unencrypted email back to the server, but overwrites it.

The e-mail server contains an e-mail application which sends an electronic envelope comprising the encrypted email and the access policy data signed by the control point box to at least one specified recipient entity. The e-mail server sends the enveloped file comprising access policy data plus encrypted e-mail to the receiving computer entities.

The receiving entities, to open and read the emails, must refer them back 907 to the control point device for decryption , i. e "opening" of the envelope. The control point device will only decrypt the email for the receiving entity, if the receiving entity can prove its identity and provided that the identity of the receiving entity is listed in the access policy data received by the control point device in the envelope with the email. The control point device compares the time of release field 1001 with an internal timer within the control point device, to see if the unencrypted e-mail can be released to the receiving entity . If e-mail cannot be released, the control point device signals to the receiving entity that the e-mail cannot be released yet. However, if the e-mail can be released, that is if the time of release specified in the access policy data is before a current time read from an internal trusted time of the control point device, then a policy enforcement engine of the control point device proceeds to check the other access policy data criteria in the other fields of the access policy data to see whether the e-mail can be decrypted and sent to the receiving entity.

The control point device reads the access policy dated to see whether that recipient is authorized, and if so, applies decryption to the document and then (optionally) re-encrypts the e-mail with the public key of the intended recipient, before sending it back 908 to the receiving entity. The control point device may also generate a receipt data, specifying that the control point device decrypted that document, and re-encrypted it with a recipients public key, at a particular time and date, and send 911 this receipt back to the originating sending entity.

The receiver can receive an email, but can only open it after a specified date listed in the access policy data. The sender has confidence that the receiver cannot open the email before the date specified in the access control policy data, and providing all other conditions specified in the access policy data are met.

Claims:

1. A method of controlling access to data stored in a database, said method comprising:

providing a secure control apparatus, said apparatus comprising a policy enforcement component for enforcing at least one data access policy to said database and a key escrow component for ensuring a set of private keys remain secure;

connecting said secure control apparatus to a web server computer entity, said web server computer entity configured for storing a plurality of encrypted files;

upon receipt of a request to access a said encrypted file, received by said web server computer entity, said secure control apparatus operating to; check for an access policy applicable to said requested file;

establish an identity of said entity requesting said file;

if said entity has an identity which, according to said access policy, is authorised for accessing said file, then releasing said file for access to said computer entity; and

if said computer entity requesting said file does not have an identity which, according to said access policy is authorised for accessing said file, then denying access of said file to said requesting computer entity.

2. A document management service comprising:

receiving a document;

receiving an access policy data describing an access policy applicable to said received document;

encrypting said document;

signing said access policy data with a digital signature of a secure device.

3. The service as claimed in claim 2, further comprising;

after encryption of said received document said secure device does not store said received document, and does not return said received document document.

4. The method as claimed in any one of the preceding claims, further comprising;

sending said encrypted document and said signed policy data to a computer entity from which said document and said access policy data were originally received.

5. A method for enforcement of an access policy applicable to a document, said method comprising:

receiving said document in encrypted format;

receiving an access policy data applicable to said encrypted document;

reading said access policy data;

verifying individual conditions specified in said access policy data;

if said individual conditions are successfully verified, then allowing decryption of said received document: and

if said individual policy requirements are not verifiable, then generating a message indicated that said encrypted document is not permitted to be accessed.

6. The method as claimed in claim 5, wherein said step of verifying said policy data comprises;

checking a time and date requirement specified in said access policy data;

comparing said time and date requirement with a time and date data generated by a secure timer device.

7. The method as claimed in as claim 5, wherein said step of verifying said access policy data comprises;

determining a requirement for auditing of a request to access said file by a third party computer entity;

receiving an authentication data identifying a user requesting access to said file;

sending said authentication data to said third party auditor computer entity;

if said third party auditor computer entity verifies said authentication data, indicating that said user is allowed to said file, then allowing the decryption of said file;

if said third party auditor computer entity does not verify that said user requesting access to said file has authority to access said file, then declining to decrypt said file.

8. The method as claimed in any one of claims 4 to 7, further comprising;

receiving a public key of a user computer entity intended for receiving said documents;

an encrypting document with said public key; and

sending said public key encrypted document to said user computer entity

9. A policy enforcement and key management device, said device comprising:

a tamper proof casing;

at least one communications port for sending and receiving electronic data; and

means for reading an access policy data; and

means for applying an access policy to a document, according to said access policy data.

10. The policy enforcement and key management device as claimed in claim 9, further comprising;

means for identifying said device.

11. The policy enforcement and key management device as claimed in claim 9 or 10, said device further comprising;

a secure timer device for generating a time and date data;

12. The policy enforcement and key management device according to any one of claims 9 to 11, further comprising;

means for detecting tampering with said device;

13. The policy enforcement and key management device as claimed in any one of claims 9 to 12, further comprising;

means for storing a list of trusted computer entities, with which said device can communicate.

14. A method for providing a service for enforcement of access policies applicable to a plurality of documents, said method comprising;

receiving at least one said document in encrypted format;

receiving at least one access policy data applicable to said encrypted document;

reading said access policy data;

determining whether a set in criteria specified in said access policy data are satisfied for said encrypted documents; and

if said set of criteria are satisfied, then decrypting said document; and making said decrypted document available to a user of said service.

15. The service method as claimed in claim 14, further comprising;

if said set of criteria are not satisfied, then denying access to said decrypted document to a user of said service.

16. The service method as claimed in claim 14 or 15, where, in said step of verifying said policy data comprises;

checking a time and date requirements specified in said access policy data;

comparing said time and date requirement with a time and date data generated by a secure timer device

17. The service method as claimed in any one of claims 14 to 16, wherein said step of verifying said access policy data comprises;

determining a requirement for auditing of a request to access said file by a third party computer entity;

receiving an authentication data identifying a user requesting access to said file; and

sending said authentication data to said third party auditor computer entity;

if said third party auditor computer entity verifies said authentication data, indicating that said user is allowed to said file, then allowing the decryption of said file;

if said third party auditor computer entity does not verify that said user requesting access to said file has authority to access said file, then declining to decrypt said file.

28

Application No: GB 0206399.8 **Examiner:** Jim Calvert
Claims searched: 5 and 14 **Date of search:** 15 October 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4A(AAP)

Int Cl (Ed.7): G06F 1/00

Other: Online: EPODOC, WPI, PAJ, TDB, XPESP, INSPEC, EXPLORE

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X,Y	EP0192243A2	(HONEYWELL) See e.g. page 28, line 9 to page 31, line 13, and also see figure 3.	X:5,14 Y:1
X	WO0079368A1	(THE BRODIA GROUP) See e.g. page 10, line 20 to page 11, line 28	X:1,5,14
X,Y	WO0025214A1	(SECURESOFT) See e.g. page 1, line 10 to page 2, line 8, page 6 lines 16 to 27 and pages 11 to 17	X:5,14 Y:1
Y	WO9605673A1	(TRUSTED INFORMATION) Whole document	Y:1

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.